Microsoft

Enabling Remote Work

A guide to enabling remote workers to stay connected, productive, and secure

Contents

Introduction

Microsoft is making public health our first priority and we are doing everything we can to help with the effects of COVID-19. We recognize the vital role our technology plays in the lives of people every day, and we want you to know that we are here to help any way we can. Like Microsoft, organizations around the world are putting the safety of their employees, customers and communities first. With stay-at-home, shelter-in-place, and similar social distancing mandates in place, many organizations have pivoted to a remote workforce.

This document provides our initial guidance for enabling a remote workforce to have secure access to the organizational information, tools, and resources they need. If your workforce is suddenly working remotely and you want to roll out software and services, use our prescriptive guidance, which is designed to help you quickly enable remote workers.

This document is primarily for IT decision makers and IT Pros who:

- Architect and build systems and solutions based on local or cloud infrastructure
- Build and maintain communication networks and systems
- Provide operational support for network systems and users, including helpdesk
- Enable or support end users who work remotely
- Manage database systems including storage, performance, and security
- Design and implement technology to support business processes and growth
- Manage device inventory, software licenses, cloud subscriptions, and vendors
- Create and implement corporate level policies and systems
- Design, test, and launch software, both internal and commercial
- Help protect information, employees, customers, and devices against security threats
- Manage user and customer identities and enforce security policies

You are not in this alone. There are many organizations who are currently faced with unexpected numbers of remote workers, and you can connect with them in the Enabling Remote Work Community.

Securing remote work

Your journey to provide a secure remote work environment depends on your starting point, but the journey for all begins with identity and delivering secure access. With the right technologies, people can be empowered to work securely from any location.

Cloud identity

The first step is to connect your on-premises identity systems to the cloud. This will enable scale, improve security, and will make working remotely easier. In a cloud-only identity model, Azure AD performs authentication. This is called cloud authentication. In a hybrid identity model, Azure AD either performs authentication or redirects the user to another identity provider, such as on-premises Active Directory Domain Services (AD DS).

In the hybrid identity model, cloud authentication is used most often (although some customers use federated authentication). In the cloud authentication model, Azure AD handles the authentication process using a locally stored hashed version of the password or by sending the credentials to an on-

premises software agent to be authenticated by on-premises AD DS. There are two types of cloud authentication:

- Password hash synchronization (PHS), where Azure AD performs the authentication itself.
- Pass-through authentication (PTA), where AD DS performs the authentication.

With federated authentication, Azure AD redirects the client computer requesting authentication to contact another identity provider. Federated authentication is primarily for large enterprise organizations with more complex authentication requirements, such as smartcard-based authentication.

Multifactor authentication (MFA)

We strongly recommend using multifactor authentication (MFA) for your users (not just remote workers, but all users, including admins). Our cloud services support a broad range of options to fit the needs of your organization and users. For security, flexibility, convenience, and cost, we recommend Microsoft Authenticator. It supports push notifications, one-time passcodes, and biometrics for any Azure AD-connected app, and it is free to download from the Apple and Google app stores.

In general, we typically recommend that users have 14 days to register their device(s) for MFA before it is required. However, if your workforce is suddenly working remotely, we recommend that you require MFA immediately as a security priority and be prepared to help users who need it. If you're hesitant to turn on MFA, there are ways to minimize disruption and make it a smooth transition for your users, but we recommend that you treat this as an emergency pilot and make sure you have support folks ready to help remote workers who get stuck.

You can get MFA a few different ways depending on your organization's needs. You may already be entitled to use MFA depending on any Azure AD, Microsoft 365, or other cloud service licenses you may already have. Basic MFA features are available to Microsoft 365 and Azure AD admins for no extra cost. And depending on when you acquired your Microsoft 365 licenses, you may already have MFA enabled for your users through security defaults that have been automatically enabled for your organization.

If you have…	We recommend that you…
Microsoft 365 (without Azure AD P1 or P2)	Enable security defaults in Azure AD

Microsoft 365 F1/3 (with Azure AD P1)	• Simplify firstline worker onboarding by integrating with core HR Systems
	• Create these conditional access policies:
	  • Require MFA for administrators
	  • Require MFA for all users
	  • Block legacy authentication

Microsoft 365 E3 (with Azure AD P1)	Create these conditional access policies: • Require MFA for administrators • Require MFA for all users • Block legacy authentication
Microsoft 365 E5 (with Azure AD P2)	Use Azure AD Identity Protection to implement these policies: • Require MFA when sign-in risk is medium or high • Block clients that don't support modern authentication • High risk users must change password

Optimizing your network for remote workers

When pivoting to a remote workforce, the sudden change in the way users connect to your organization can have an adverse effect on your network infrastructure, which in turn will cause poor performance

and a poor user experience. The most common network design we see used by our customers is illustrated below.

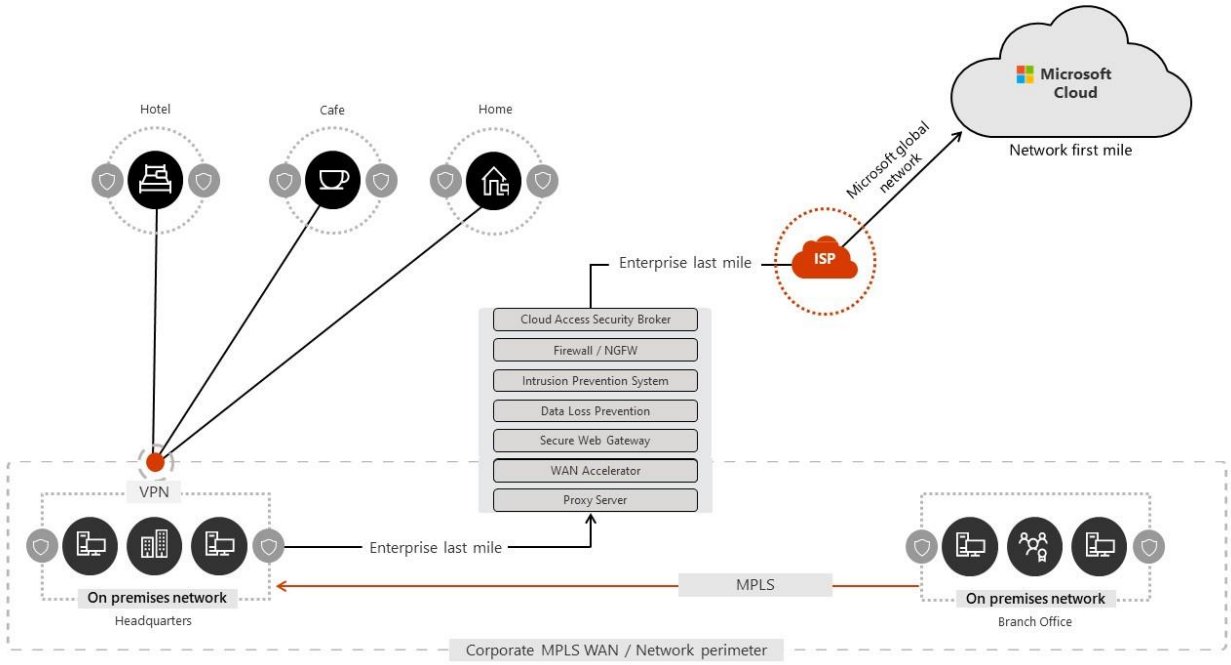

Figure 1 - Common enterprise network

This design works very well when the majority of applications, data and services are on the organization's network. But it doesn't work well in situations where the majority of remote worker traffic goes into and out of the corporate network to reach cloud resources. Many customers have told us that they have seen a rapid shift in network traffic which used to be contained within the organization network now almost exclusively connecting to some cloud-based endpoint.

We have been working closely with customers and the wider industry for years to provide effective, modern solutions to these problems that are aligned to industry best practices and apply equally and effectively to remote workers as they do to branch offices. As a result, there are two simple steps you can take to drastically reduce the adverse effects on your internal network infrastructure when a large percentage of your users are working remotely at once:

1. Identify the endpoints that need to be optimized; and
2. Optimize the identified endpoints.

For step 1, Microsoft has already identified for you the endpoints that need to be optimized. In the URL/IP list these endpoints are marked as "Optimize." For step 2, you need to configure your VPN clients for split tunneling to the endpoints marked as Optimize, which will divert these endpoints away from the VPN tunnel and allow the user to connect directly to them from their home Internet connection.

As part of our response to the COVID-19 outbreak, we have declared a temporary moratorium on some planned URL and IP address changes for Microsoft 365. This is intended to provide customers with confidence and simplicity for implementing these two steps. From March 24, 2020 through June 30,

2020 we will halt changes to IP ranges and URLs included in the Optimize category. Changes within other endpoint categories will occur as usual. During this period, you can use Optimize category service endpoint definitions in a static manner to perform targeted network optimizations (such as bandwidth reservations and split tunnel VPN configuration) with minimal risk to cloud connectivity due to cloud-side network changes. After the moratorium period, we recommend that you implement change management and/or automation processes for Microsoft 365 service endpoints using this guidance.

Secure access to apps

In addition to providing cloud authentication for users, Azure AD can also be your single control plane to secure all your apps, whether they're on-premises, in Microsoft's cloud, or in another cloud. Using Azure AD to sign into apps isn't just about being more secure. It's also about being more productive. Our customers use about 180 apps on average—and this number keeps growing. By integrating your apps into Azure AD, you can make it easy for remote workers to discover the applications they need and sign into them securely. Using the Azure portal, you can find more than 3000 SaaS applications in the App Gallery and configure them for single sign-on with just a few clicks. You can automatically provision and de-provision access to the apps so that people who need them can start using them right away.

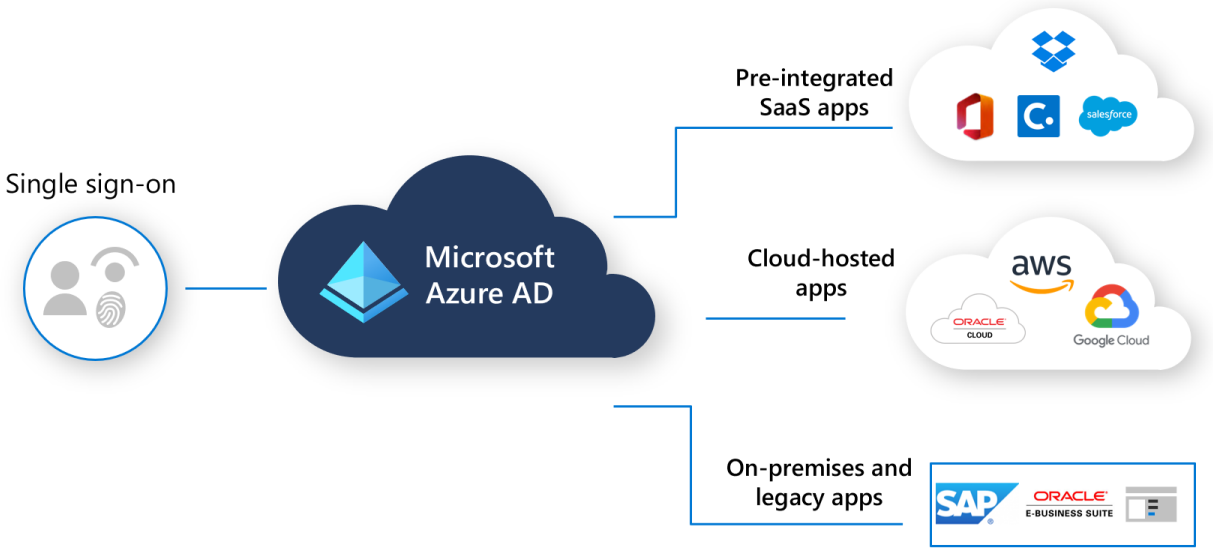

Figure 2 - Azure AD provides secure single sign-on access to on-premises and cloud apps

When you connect your apps to Azure AD, your remote workers need only sign in once to access them, and they need only one set of credentials. To make on-premises web apps available without a VPN, you can use Azure AD Application Proxy, while tools from our secure hybrid access partners can provide access to legacy apps. To get productive from wherever they are, a remote worker simply goes to the My App Portal, where they can find all the apps they have permission to use.

To protect your organization, it's essential that when you enable access to cloud apps from personal devices and remote locations, it is done securely. Azure AD Conditional Access can be used to apply security policies to help ensure the right people have access to the apps they need, in line with your organizational requirements. You can extend your policies to protect all apps, requiring controls like passing an MFA challenge or using a compliant device. We recommend you examine your policies and

ensure they're not preventing remote access. Policies that block access when off the corporate network are common and could cause problems. You may find that an alternative combination of Conditional Access controls will enable remote work, while still meeting your security requirements.

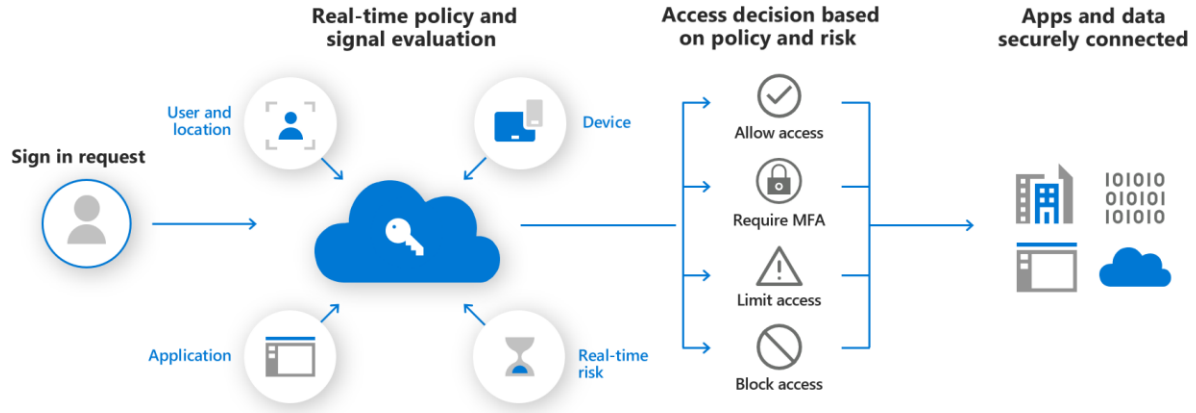

Figure 3 - Apply consistent risk-based policies with Conditional Access

If you're not using Conditional Access, security defaults can help keep your users and apps secured. Microsoft has made security defaults available to everyone to ensure that all organizations have a basic level of security enabled at no extra cost. You turn on security defaults in the Azure portal, as shown below.

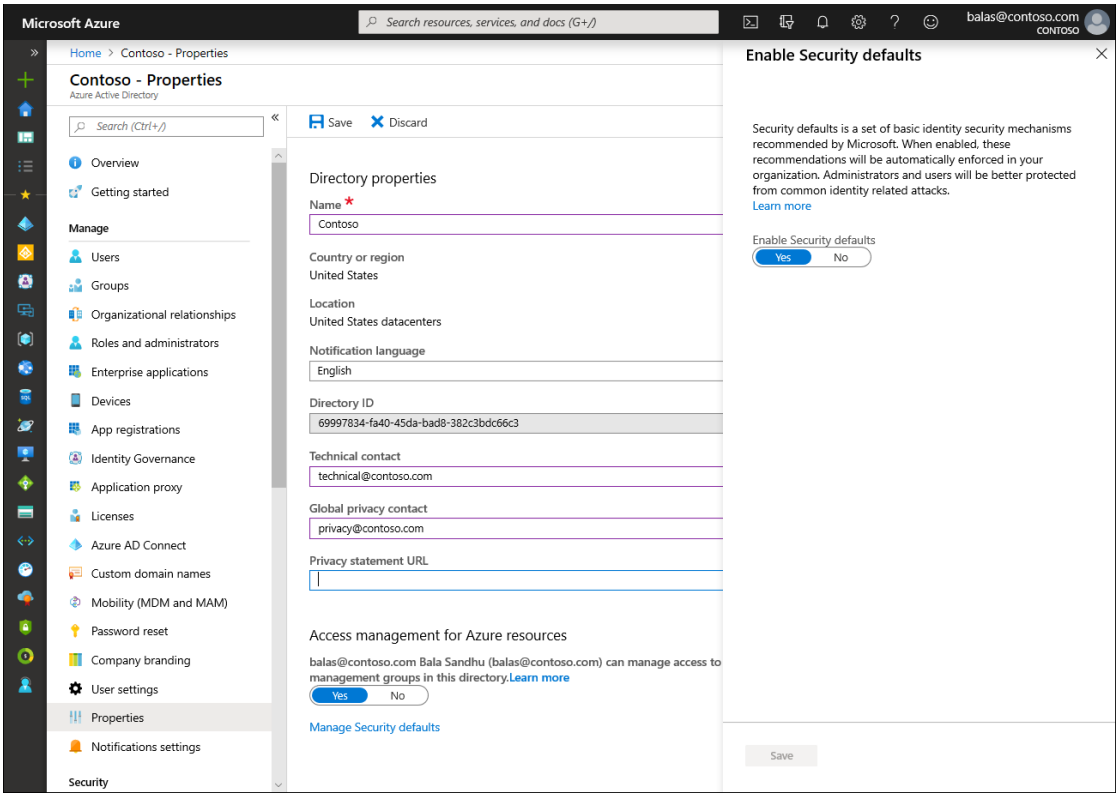

Figure 4 - Enable security defaults in the Azure portal

Some organizations run several business-critical apps on-premises that are not accessible from outside the corporate network. You can use Azure AD Application Proxy to provide secure access to on-premises apps to your remote workers without the need for a virtual private network (VPN) or dual-homed servers and firewall rules. Azure AD Application Proxy is a lightweight agent that enables Internet access to your on-premises apps, without opening up broad access to your network. You can combine this with your existing Azure AD authentication and Conditional Access policies to help keep your users and data secured.

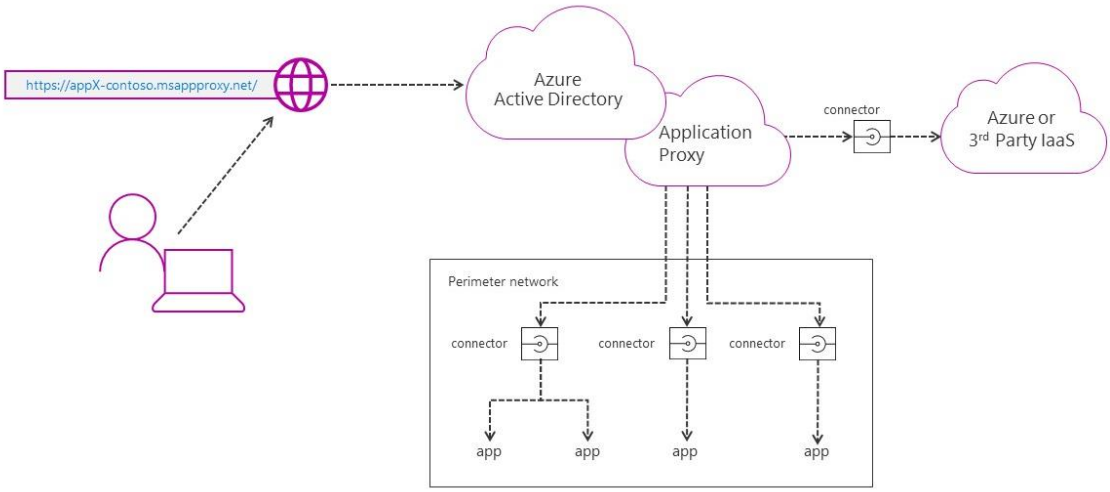

Figure 5 - Application Proxy enables remote workers to connect to apps without a VPN or dual-homed servers and firewall rules

A VPN provides another secure way for remote workers to connect to their organization's network. This is especially useful for remote workers using public Wi-Fi. The Azure Point-to-Site (P2S) VPN is cloud-based and can be provisioned quickly to accommodate a sudden increase in demand from users working at home. It can scale up easily and be turned off just as easily and quickly when the increased capacity is not needed anymore. A P2S VPN gateway connection lets you create a secure connection to your virtual network from an individual client computer.

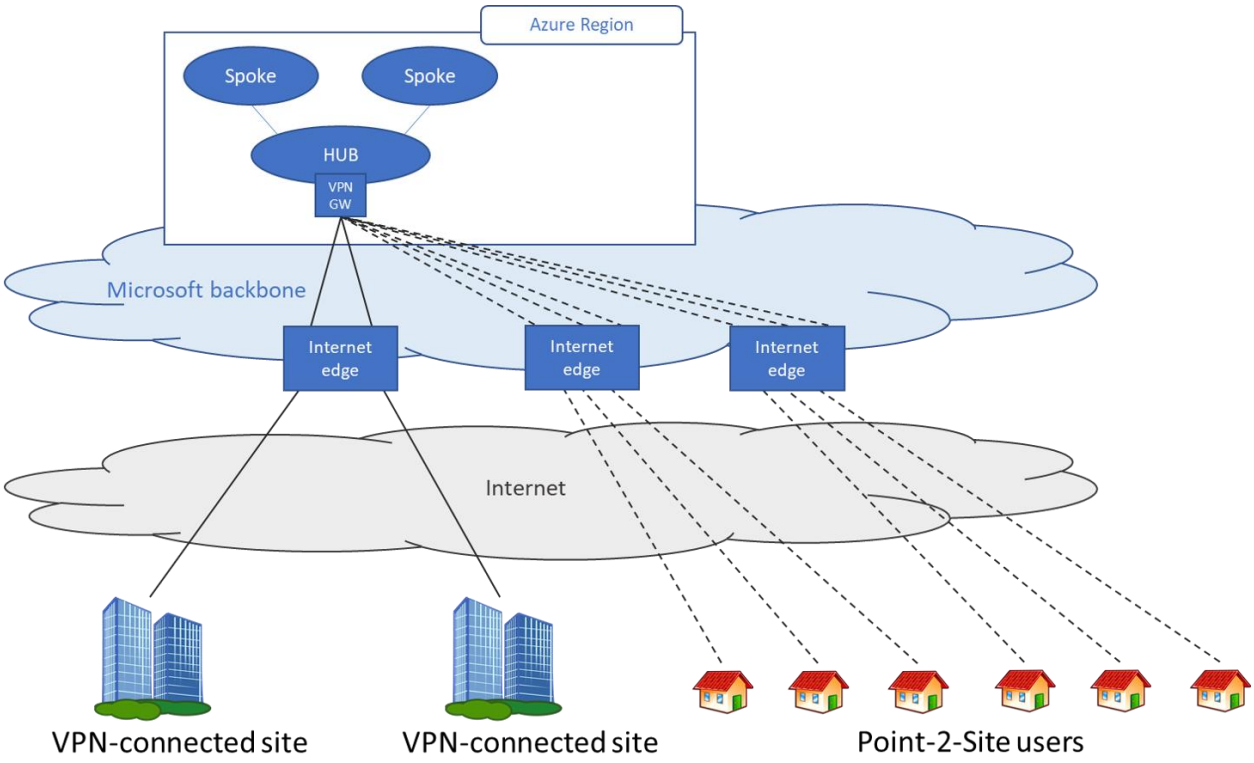

Figure 6 - Azure P2S VPN can be provisioned quickly to accommodate a sudden increase in demand from remote workers

A P2S connection is established by starting it from the client computer. This solution is useful for workers who want to connect to Azure VNets and/or on-premises datacenters from a remote location. For enterprises and organizations looking to optimize and scale out their VPN capabilities, in addition to the network guidance provided above, some additional best practices recommended by Microsoft are:

- Collect user connection and traffic data in a central location for your VPN infrastructure, use modern visualization services, like Power BI, to identify hot spots before they happen, and plan for growth.
- If possible, use a dynamic and scalable authentication mechanism like Azure AD to avoid the trouble of certificates.
- Improve security using MFA if your VPN client is Active Directory-aware like the Azure OpenVPN client.
- Geographically distribute your VPN sites to match major user populations, use a geo-load balancing solution such as Azure Traffic Manager, to direct remote workers to the closest VPN site and distribute traffic between your VPN sites.
- Instead of allowing full 24 x 7 access to on-premises servers, use Just-In-Time (JIT) VM access instead. Make sure to also review the Secure management ports control in Azure Security Center and remediate the recommendations that are relevant for this scenario.
- Some workloads (servers, containers, databases) that will be accessed by remote workers might be missing critical security updates. Review the remediate vulnerabilities control in Azure Security Center to prioritize the updates that must be installed. Make sure to review the result of all recommendations in built-in vulnerability assessment and remediate those items.

Windows Virtual Desktop (WVD) can be used to provide secure access to on-premises apps. WVD is a comprehensive desktop and app virtualization service running in the cloud. It's the only virtual desktop infrastructure that delivers simplified management, multi-session Windows 10, optimizations for Office 365 ProPlus, and support for Remote Desktop Services. It allows you to deploy and scale your Windows desktops and apps on Azure in minutes with built-in security and compliance features.

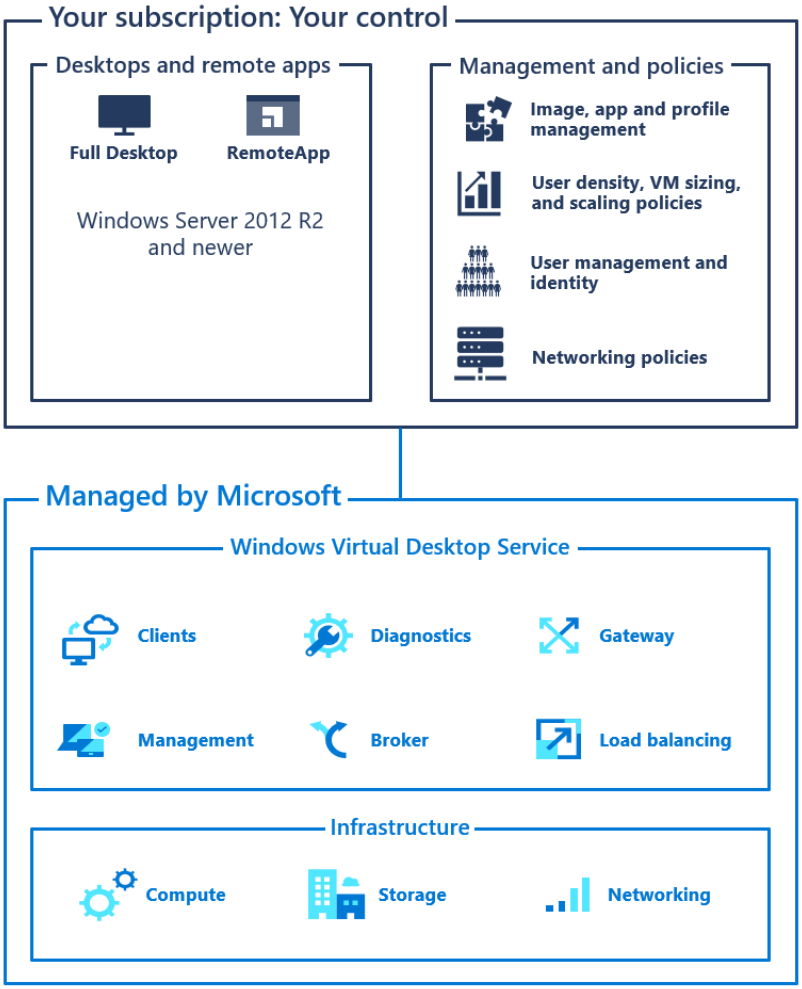

Figure 7 - Windows Virtual Desktop helps simplify management, provisioning, and access to corporate data and apps

Remote Desktop allows you to connect to a PC at a remote location. For example, remote workers can use Remote Desktop to connect to a PC on their organization's network from their Windows, iOS or Android device. Once you are remotely connected to a workplace computer, you can use it as if you were sitting in front of it.

Microsoft Secure Score

Secure Score is a measurement of an organization's security posture, with a higher number indicating more improvement actions taken. Following Secure Score recommendations can protect your organization from threats. Secure Score can help you report on the current state of your organization's security posture, improve your security posture by providing discoverability, visibility, guidance, and control, and enable you to compare your score with benchmarks and establish key performance

indicators. Secure Score is available from a centralized dashboard in the Microsoft 365 security center, and the Secure Score page of the Azure Security Center.

Empower remote workers

To be productive, people need to communicate and collaborate with one another. They need to meet, chat by voice and text, and share information and files. To keep teams connected while they work apart, get Microsoft Teams and Microsoft 365 available to as many people as possible.

Microsoft Teams

Teams allows you to chat, meet, call, and collaborate all in one place. Millions of people get their work done in Teams every day because it brings together everything you need to work remotely into a hub for teamwork. Teams has clients available for desktop (Windows, Mac, and Linux), web, and mobile (Android and iOS).

Chat and conversations

Chat and threaded conversations are at the center of Teams with support for individual 1:1 chats and group chats and conversations. Remote workers can share information, opinions, and personality by using gifs, stickers, and emojis in group chats or one-to-one messages.

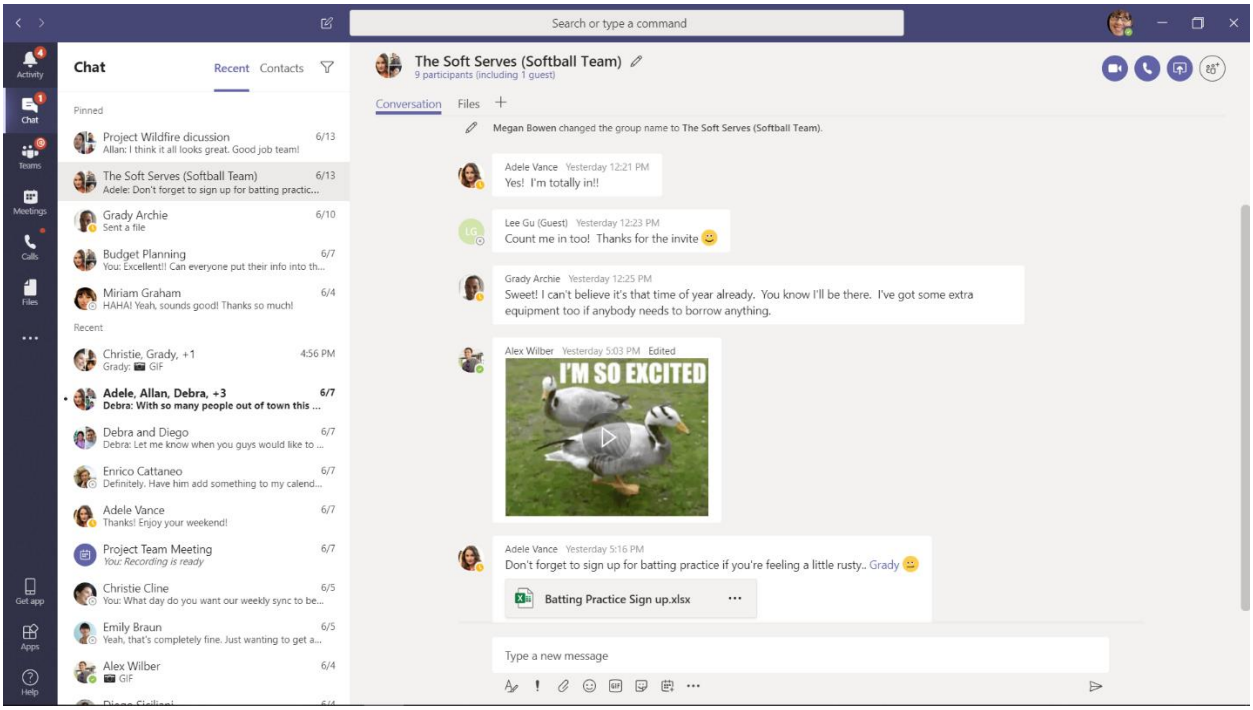

Figure 8 - Chat and threaded conversations are at the center of Teams

Meetings and conferencing

Teams can certainly help maintain communications and information sharing with remote workers, especially with meetings that support up to 250 people. Teams meetings enable interactive, collaborative meetings with people inside and outside your organization. Remote workers can use Teams meetings for day-to-day activities including recurring project checkpoints, catching-up with colleagues, brainstorming sessions, and facilitating conversations with customers. Companies and

schools also use Teams meetings to support remote learning and training with both internal and external audiences. As a result of the COVID-19 outbreak, Microsoft has shifted to a remote workforce and is using Teams to keep our remote workforce connected and productive. You can use this article for guidance on supporting your remote workers with Teams.

Teams meetings allow remote workers to:

- Invite people from inside or outside the organization (up to 250);
- Designate presenters and attendees to provide more formal meetings or classes;
- Talk with video and chat, and collaborate in real time with screen sharing and digital whiteboards;
- Stay in the know before, during, and after meetings with a meeting lifecycle;
- Follow along in meetings with live captions;
- Remove visual distractions with custom background effects and unwanted background noise with real-time noise suppression (coming soon);
- Catch up on missed meetings with recordings and searchable transcripts;
- Join meetings from any browser or from the Teams app on a PC, Mac, Linux, iOS, or Android device;
- Join meetings from a phone when their Internet connectivity is poor or unavailable; and
- Use the Bookings app to schedule, manage, and conduct virtual appointments (for example, a healthcare provider following up with a patient post-surgery).

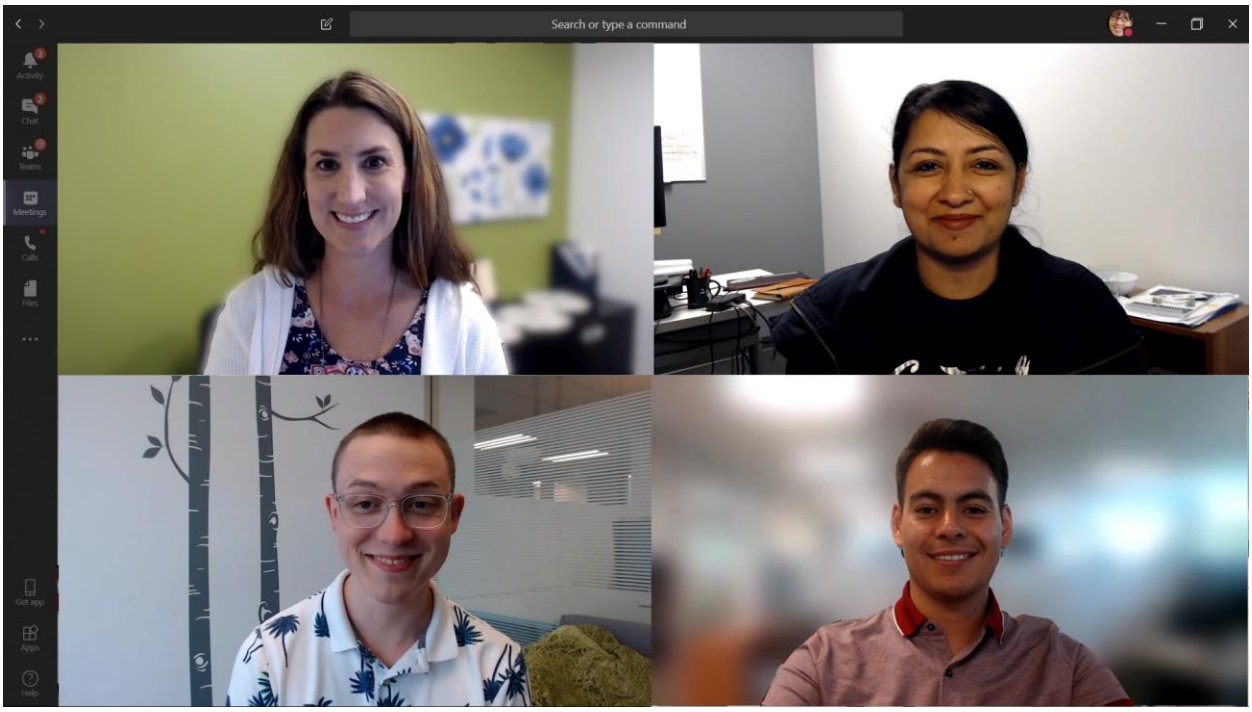

Figure 9 - Teams provides a great out-of-the-box experience for online meetings & video conferencing

Seamless integration between Outlook's calendar and Teams meetings enables users to schedule and join Teams meetings directly from Outlook. If all your mailboxes are in Exchange Online, this integration is automatic. If you are in an Exchange hybrid configuration, you may need to enable users to create Microsoft 365 Groups, as Groups are used by Teams. If all your Exchange mailboxes are on-premises, you need to enable some Exchange hybrid features. You don't have to move all your mailboxes to Exchange Online to get immediate benefits. In fact, with the Exchange Hybrid Agent you can be Hybrid with Exchange Online in minutes, and be able to start scheduling Teams meetings straight from Outlook.

Calling

Teams supports direct VoIP calling between users and even other organizations using federation. It uses the same codecs as meetings and provide great audio world-wide without additional PSTN charges. However, some users may need a dedicated phone number to take external calls when working remotely. Teams can quickly provide cloud phone service for these users to make and receive phone calls.

Start with Phone System, the Cloud PBX that was built for Teams. To provide dial tone, add a Microsoft calling plan and quickly issue phone numbers to your staff. You can also port existing numbers. These services are provided and supported by Microsoft.

If you want to keep your existing telecom providers, consider using Direct Routing that comes with Phone System. This allows you to connect your existing calling trunks directly to Teams. We have several partners who can engage and help with these deployments. These two options for dial tone are mix and match – you can have calling plans for quick deployments and use Direct Routing for larger and more custom approaches. Together they provide nearly world-wide coverage where we offer Phone System.

Calling Plans and Direct Routing both support more than 35 key features for users including Cloud Voicemail, Call Forwarding, and send/receive delegation.

Content collaboration

For content collaboration, Teams provides remote workers with a central place in the cloud to store and share files with OneDrive and SharePoint, co-author, communicate, and collaborate. Remote workers can also securely work from anywhere with the Office and Teams mobile apps.

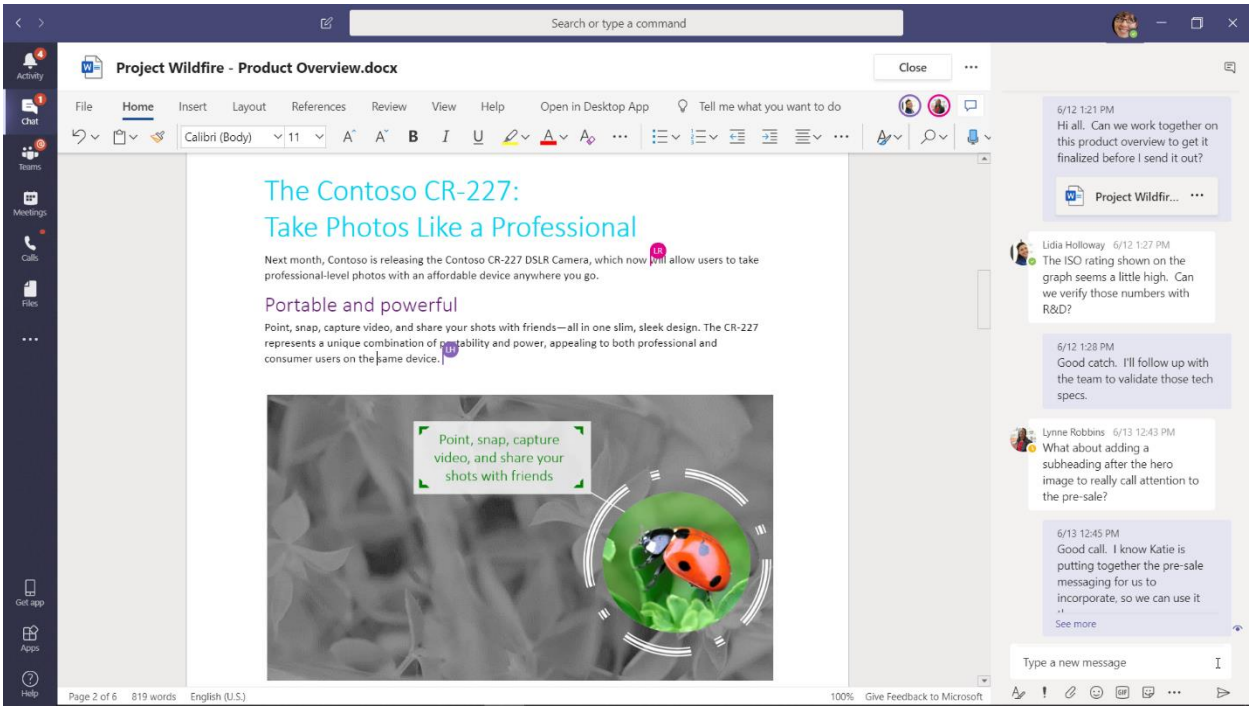

Figure 10 - Teams provides a central place to share files, co-author, communicate, and collaborate

Apps and workflows

Teams provides a platform for apps and workflows that can be accessed from the desktop, web, and mobile versions of Teams. Teams provides hundreds of apps published by Microsoft and by third parties to engage users, support productivity, and integrate commonly used business services into Teams. Users and Admins can also create custom apps and automated workflows for Teams using the low-code Power Apps and Power Automate development tools.

Apps and workflows let remote workers be more productive in Teams, by collecting and sharing critical information, automating repetitive tasks, and allowing them to chat with interactive bot. Pinning apps to a channel or the Teams app bar is a great way for users to make these apps easily accessible in a relevant space, and admins can pin apps to drive awareness and adoption of the apps that everyone should be using.

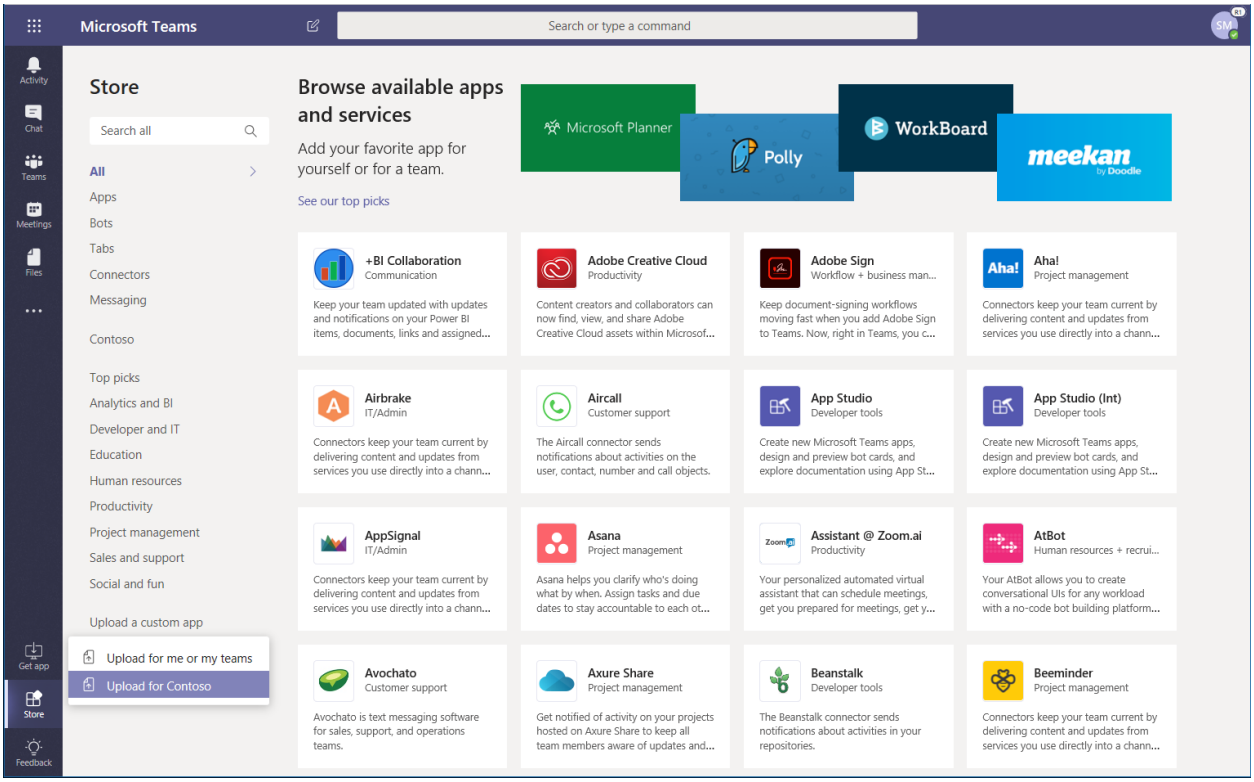

Figure 11 - Apps let remote workers do more in Teams

Teams for firstline workers

We've made Teams the hub for teamwork for all workers, providing a single productivity experience that connects all levels of the organization from the c-suite the firstline. We also recognize that Firstline Workers have some unique needs and requirements. As such, we've shaped the Teams experience to effectively meet the core technology needs of Firstline Workers and we continue to add new firstline features to build a purpose-built experience. We also have resources available to accelerate the enablement of Firstline Workers with Teams, including a Quick Start Guide and details on how to provision and manage Teams for Firstline Workers at scale.

Get started with Teams

There are several ways to get Teams:

- If you have Microsoft 365 or Office 365, you already have Teams.
- If you work for a business that isn't currently licensed for Teams, you can use the free Office 365 E1 offer for six months.[1] Contact your Microsoft partner or sales representative to get started today.
- If you don't have Microsoft 365, Office 365, or a current license for Teams, you can use the Freemium version of Teams for free.
- If you work in education and want to set up teachers, students, and administrators on Teams, sign up for Office 365 A1. This free version of Office 365 is available to all educational institutions.

[1] Not available in GCC High or GCC DoD.

- End users at organizations with a Microsoft cloud account can use the Teams Exploratory Experience to initiate a Teams experience (admins can switch this feature on or off for users in their organization), even if they are not currently licensed for Teams.

If you have Teams, VoIP calling is already available. If you haven't already done so, we recommend that you explore your options for federation so you can call other organizations who use Teams. If you need to make and receive traditional phone calls, add Phone System and calling plans to issue dedicated phone numbers to users. For larger deployments, explore Direct Routing.

To get started quickly on Teams, we recommend you create two or three teams and channels for a select group of early adopters. By first rolling out Teams on a small scale, you'll learn Teams by it and gain valuable insight to help you deploy Teams across your whole organization. Start with chat, teams and channels, and meetings. If you're a large organization with a hybrid or on-premises Skype for Business configuration, or if you want to roll out voice features, use our get started guidance and the deeper adoption guidance.

External access is a way for Teams users from an entire external domain to find, call, chat, and set up meetings with your organization's users in Teams. You can also use external access to communicate with external users who are still using Skype for Business (online and on-premises) and Skype (in preview). If you want external users to have access to teams and channels, guest access might be a better way to go. For more information about the differences between external access and guest access, see Compare external and guest access.

Microsoft 365

You can provide familiar productivity apps to your users and enable teams within your organization to work together seamlessly across different locations. Office gives people the tools to collaborate in real time, securely share files, and easily communicate with teammates from anywhere and on any device. As long as they can connect to the Internet, your users can connect to the files and people they need to stay productive, and with the advanced security features built in, their data is protected by enterprise-grade security.

Like workers in the office, remote workers need to be able to check their email, manage their time and calendars, access documents, work as part of a team and continue with their usual activities. Microsoft 365 and Microsoft Office give people the tools they need to organize their day, collaborate in real time, securely share files, and communicate with teammates from anywhere and on any device. As long as they can connect to the Internet, your users can find and connect to the information, files and people they need to stay productive, and with the advanced security features built in, their data is protected by enterprise-grade security. We have Microsoft 365 plans and experiences built for all workers from the c-suite to the firstline.

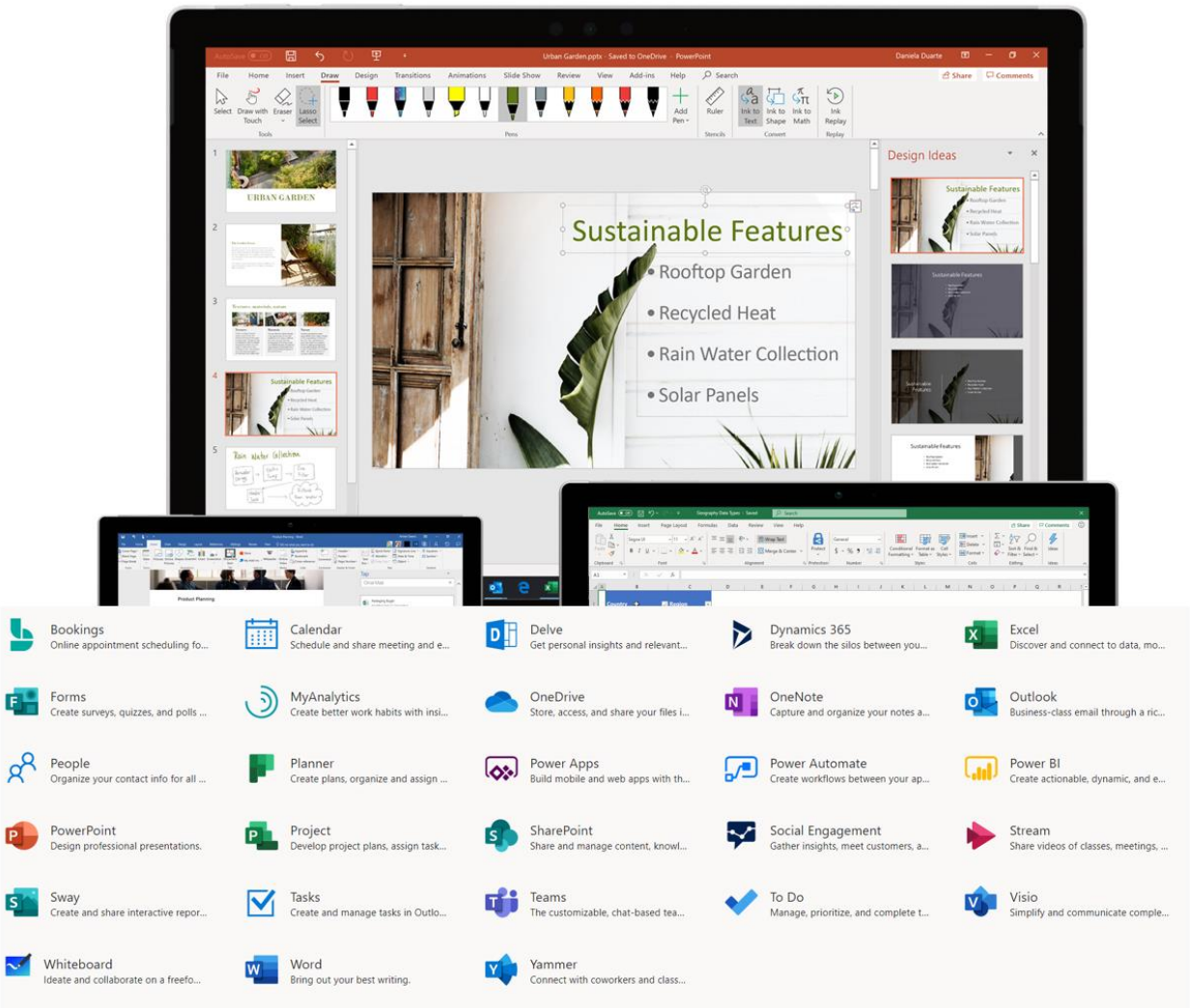

Figure 12 - Microsoft 365 and Microsoft Office give people the tools they need to work from anywhere and on any device

Office 365 ProPlus is the most productive and most secure Office experience for enterprises, allowing people to work together seamlessly from anywhere, anytime. Remote workers can collaborate on a document with multiple people simultaneously, see edits and changes in real time, and coauthor with others on any laptop, PC, or mobile device. They can log in to office.com to find their documents, pick up where they left off, and use Word, Excel, PowerPoint, Outlook, and other apps from almost any browser. They can invite conversation and collaboration with @ mentions and threaded comments and they can collaborate with their team on the same digital canvas using Microsoft Whiteboard.

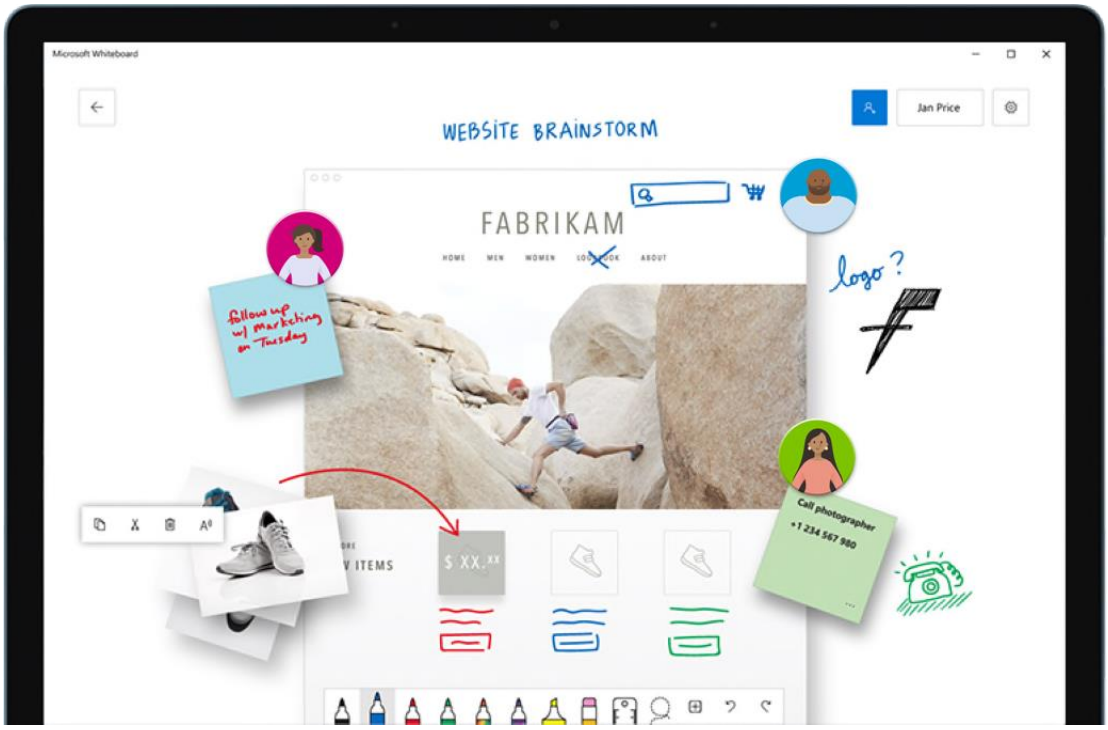

Figure 13 - Microsoft Whiteboard can bring your team together on the same virtual canvas, around the world and across devices

With Outlook, remote workers can stay connected and organized with email, calendars, contacts, tasks, and more—together in one place. Outlook helps you stay on track and prioritize your day based on what's relevant to you. Outlook enables you to share attachments right from OneDrive, plan and join Teams meetings, view and share calendars, and provide delegate permissions to others. Knowing what's coming up next across both work and personal commitments and what needs attention can help remote workers focus on what matters. Outlook provides helpful ways for remote workers to manage their time and to find what they need easily, including files, people in the organization, and more. Available for the Windows and the Mac, and for the web and iOS and Android devices, Outlook and Microsoft 365 are trusted to provide security that protects your privacy and keeps your data safe.

Microsoft Search is a new enterprise search experience that increases productivity and saves time by delivering more relevant search results. With Microsoft Search, remote workers can find and discover information to help them stay informed, learn what their colleagues have been working on, and see what's been shared with them. They can click the search box across Microsoft 365 and instantly find people, news, and documents that are important to their work, or find a colleague or coworker with simple search syntax like "Jane the engineer in London."

Regulated industries face unique challenges as they enable remote work while protecting data and complying with regulations. The security and compliance features built into Microsoft 365 can help regulated organizations balance these imperatives while meeting their core objectives. For example, healthcare teams can securely share and protect patient data, enabling them to deliver their best care at the point of care. Virtual visits using Teams can enable compliance and empower clinicians to deliver their best care. In the public sector, cross-agency collaboration and remote governance require the flow and protection of data–including highly sensitive data—on a massive scale. With Microsoft 365, governments can take immediate steps towards a Zero Trust security model. Finally, Microsoft 365 can

support financial institutions to enable remote work with productivity and security services that allow employees to harness data outside of the organization network.

Get started with Microsoft 365

You can get Microsoft 365 or Office 365 a number of ways:

- Free 6-month trial versions of Office 365 for our commercial cloud and Office 365 GCC.
- Free version of Office 365 for new and existing education and non-profit customers.
- A variety of free trials for Microsoft 365 are also available, including Microsoft 365 Business, F1, F3, E3, and E5.

Microsoft has compiled an easy-to-follow how-to downloadable adoption guide that walks you and your team, step-by-step, through the best way to roll out Microsoft 365 to your organization. The insights we share come from our most successful customers, who have maximized the power of their investment, adopting multiple, integrated technologies that now form Microsoft 365. There are many organizations who are currently launching Microsoft 365 technologies and you can connect with them in the Driving Adoption Community.

There are several options for deploying Office productivity apps to remote workers, as detailed in the following table.

Scenario	Options	Resources
Unmanaged devices (e.g., home computers)	• office.com (browser-based access) • Home install of Office 365 ProPlus • WVD with Office 365 ProPlus	Office for the web Office for the web service description
Unenrolled mobile devices	• Office mobile apps • office.com (browser-based access) • Outlook for iOS and Android	Office app - iOS / Android Outlook - iOS / Android OneDrive - iOS / Android Yammer - iOS / Android Teams - iOS / Android Microsoft 365 mobile apps
Managed devices (mobile and desktop)	• Office 365 ProPlus • office.com (browser-based access) • Outlook	Deploy Office 365 ProPlus to remote workers Configuring Office 365 ProPlus updates for remote workers using VPN Office 365 ProPlus Office deployment tool Deploy Office 365 ProPlus using Remote Desktop Services Deploy Office 365 ProPlus with an OS image Deploy Outlook mobile

Whether you use managed or unmanaged devices, the Office cloud policy service enables you to enforce policy settings for Office 365 ProPlus on a user's device, even if the device isn't domain joined or otherwise managed. When a user signs into Office 365 ProPlus on a device, the policy settings roam to that device. You can also enforce some policy settings for Office for the web, both for users who are signed in and for users who access documents anonymously.

Enable remote desktop access

The COVID-19 outbreak highlights not only the need for remote access, but also for remote desktop access. As noted above, WVD can provide access to on-premises apps through app virtualization, but it can also provide remote access to critical virtual desktops. WVD helps remote workers be productive with a virtualized experience on a PC, phone, tablet, or browser. It also enables you to simplify

management, provisioning, and access to corporate data and apps; reduce the costs and resources associated with managing on-premises infrastructure; and empower IT to transform the workplace.

WVD leverages Azure and Microsoft 365 to deliver productivity solutions for remote work. Windows 10 and Office 365 are automatically kept up to date, and IT is equipped with cloud-connected management powered by Microsoft Endpoint Manager. This provides organizations with the most productive and most secure computing experience for users while lowering total cost of ownership and reducing complexity for IT teams.

Get started with WVD

You can get WVD a number of ways:

- Activate an existing Windows 10 Enterprise E3 license for your tenant. If you don't have a Windows 10 E3 license, ask your Microsoft Account team about getting started with a free 6-month trial.[2]
- Set up or use an existing Azure AD tenant associated with your Azure subscription or your Microsoft 365/Office 365 tenant. If you don't have an Azure account, get started with an Azure free account.
- Review the Getting Started technical documentation. If your organization uses on-premises resources, review the network guidance.
- Visit the Azure Migration Center for video guidance on migrating desktops and apps to Azure using Azure Migrate, which can also help you assess your sizing needs and estimate deployment costs.
- Learn about and how to deliver remote desktops and apps from Azure with Windows Virtual Desktop.

If you want to…	We recommend that you…
Ensure security and regulation	Set up a free Azure account for use with WVD, Citrix, or VMware deployments and get ready to deploy by reviewing the Azure Academy Quick Start videos.
Adjust to a flexible workforce	Review the WVD technical documentation and network considerations.
Run specialized workloads	Migrate desktops and apps using the Azure Migration Center and attend the WVD Virtual Event (March 2020).

Manage devices, PCs and endpoints

With many people shifting unexpectedly to remote work, IT needs to support a growing number of personal devices. Endpoint management is a policy-based approach to security that requires devices to comply with specific criteria before they are granted access to resources. Microsoft Endpoint Manager delivers a modern workplace and modern management capabilities to keep your data secure in the cloud and on-premises. Endpoint Manager provides services and tools for managing mobile devices, desktop computers, virtual machines, embedded devices, and servers by combining services you may already know and be using, including Microsoft Intune, Configuration Manager, Desktop Analytics, co-management, and Windows Autopilot.

[2] The trial has a user limit of 25 seats per code - extensions available for larger deployments beginning April 1, 2020.

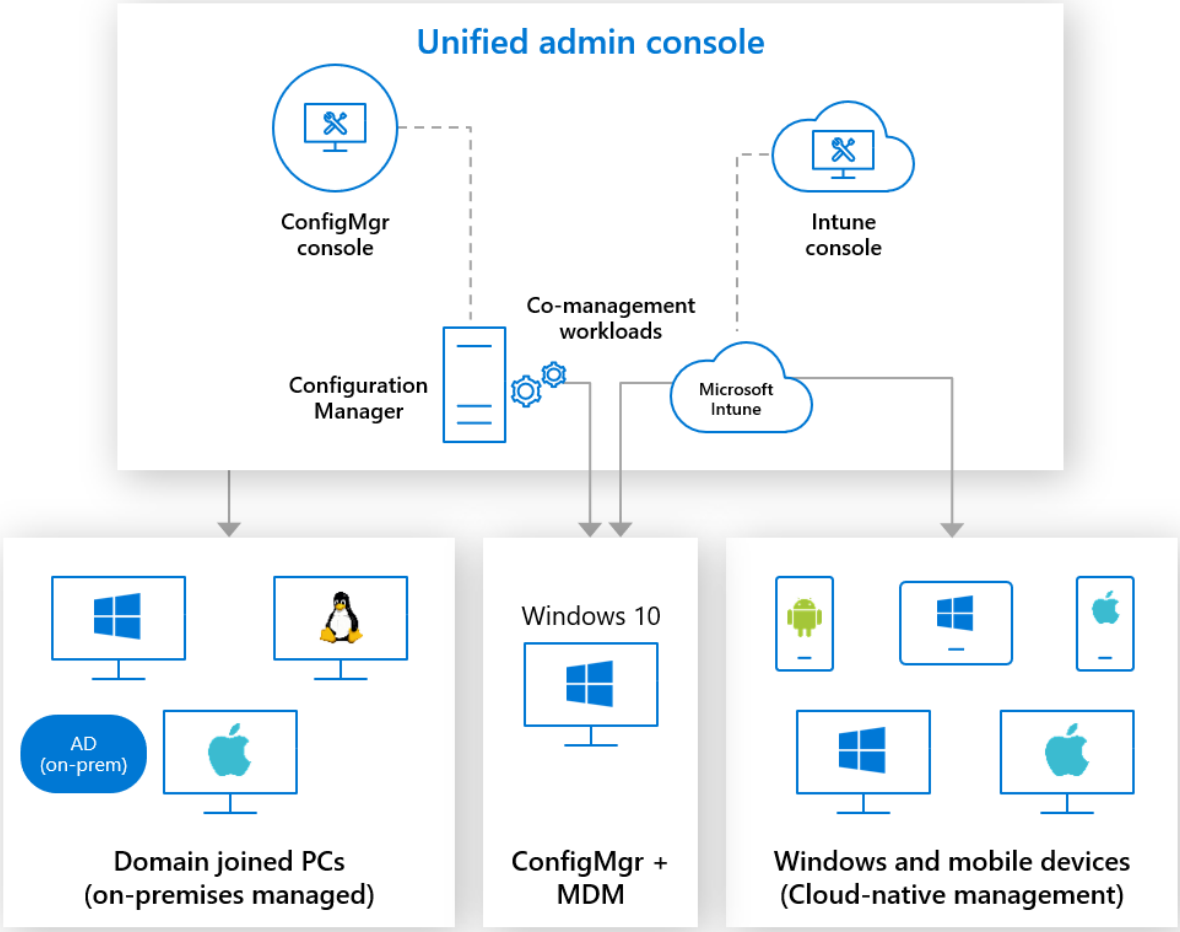

Figure 14 - Microsoft Endpoint Manager delivers modern management to keep your data secure in the cloud and on-premises

Microsoft Intune

Intune is designed to help you safeguard data when you don't manage the devices used to access organization data. Intune app protection policies combined with Azure AD Conditional Access provide granular control over data on mobile devices. Intune also enables you to define comprehensive policies that allow only the right people under the right conditions to access your company data and ensure the data stays protected by controlling how they use it within Office, Outlook and other mobile apps.

Configuration Manager

Configuration Manager is an on-premises management solution to manage desktops, servers, and laptops that are on your network or internet-based. You can cloud-enable it to integrate with Intune, Azure AD, Microsoft Defender ATP, and other cloud services. Use Configuration Manager to deploy apps, software updates, and operating systems. You can also monitor compliance, query and act on clients in real time, and much more.

Desktop Analytics

Desktop Analytics is a cloud-based service that integrates with Configuration Manager and provides you with insight and intelligence so you can make informed decisions about your Windows clients. It

combines data from your organization with data aggregated from millions of devices connected to Microsoft cloud services. With Desktop Analytics, you can create an inventory of apps running in your organization, assess app compatibility with the latest Windows 10 feature updates, identify compatibility issues, and receive mitigation suggestions based on cloud-enabled data insights, create pilot groups that represent the entire application and driver estate across a minimal set of devices, and deploy Windows 10 to pilot and production-managed devices.

Windows Autopilot

Windows Autopilot is a zero-touch, self-service Windows deployment platform. It includes a collection of technologies used to set up and pre-configure new devices, getting them ready for productive use. You can also use Windows Autopilot to reset, repurpose and recover devices. This solution enables an IT department to achieve the above with little to no infrastructure to manage, with a process that's easy and simple. From the user's perspective, it only takes a few simple operations to make their device ready to use. From the IT pro's perspective, the only interaction required from the end user is to connect to a network and to verify their credentials.

Get started with endpoint management

There are a few ways to determine the next steps for your organization, but ultimately, your next steps depend on what your organization needs. For example, start with Intune if you're are using MDM or MAM, or if use ADMX templates to control Office, Edge, or Windows settings. We also recommend starting with Intune if you have limited or no management tools/capabilities, or if you add rules and control settings for your users, apps, and devices. You can sign up for a free Intune trial here or a free Intune trial for education customers here.

If you currently…	We recommend that you…
Have significant, complex existing on-premises infrastructure	Connect your Configuration Manager site to Intune for instant value. If you are licensed for Configuration Manager, you're also licensed for Intune to co-manage your Windows 10 PCs at no extra cost.
Deploy apps and want to use conditional access based on security requirements	Start with Co-management.
Are responsible for keeping Windows 10 devices up to date	Start with Desktop Analytics.
Constantly provision new devices	Start with Windows Autopilot. Use this walkthrough to test Windows Autopilot on a virtual machine or physical device with a free 30-day trial premium Intune account.

Organizational communications

In any situation, communication across an organization is important for maintaining a healthy work culture and managing change. When an organization’s workforce is remote, especially unexpectedly, effective organization-wide communication becomes critical. Regardless of geography or industry, a common challenge all organizations face when responding to crises, is determining how best to share real-time information and provide a platform for employees to connect.

Email

Email is one of the most ubiquitous means of communicating and a great way to communicate for and with remote workers. In fact, access to email from outside the organization was practically the original remote worker feature. In today’s modern world, email remains ever important for communications.

Exchange Online supports a variety of clients, enabling your remote workers to communicate on any operating system and device type.

It's likely that your users are accustomed to using email today, but in times of crisis, it's important to keep messages to the point and not overwhelm people with large or unnecessary emails. Some ways to prevent unnecessary emails are to prevent reply-all storms, restrict who can send to large distribution lists, and adjust recipient limits.

Live events

Communication can take place in online meetings and live events. While these might sound similar, there's a key distinction. An *online meeting* is the virtual equivalent of what happens in a conference room when people come together and work together in real time. A *live event* is the virtual equivalent of what happens in an auditorium when one person or a few people communicate to a large group with an event experience and controlled content.

During times of potential business disruption organizations look to deliver large scale messaging to employees as a part of business continuity communications. Even in the absence of a crisis, organizations need to engage employees to manage change and drive culture and keep people informed with news and announcements, company-wide events, and custom experiences. Microsoft 365 Live Events includes Teams, Yammer, and Microsoft Stream and delivers highly scalable real-time video delivery of communications with the capacity to facilitate live Q&A and more. To help support our customers, through July 1, 2020, we are temporarily enabling larger private and public events through our live events assistance program. Up to 100,000 people from inside or outside your organization can watch the live broadcast through a custom-produced live event.

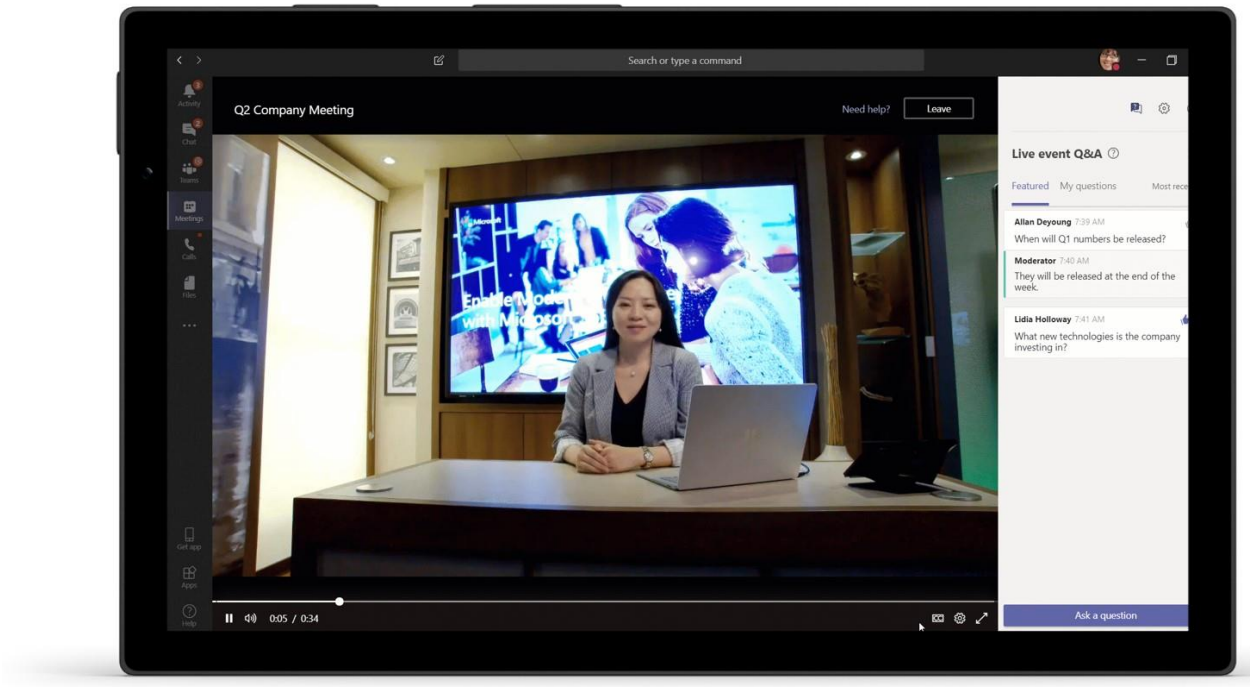

Figure 15 - Live Events delivers highly scalable real-time video delivery of communications that includes live Q&A and more

Whether you choose to host an event in Teams, Yammer, or Stream will depend on the format, purpose, and audience of your presentation.

If you want to…	We recommend that you…
Structure and deliver large broadcast-style internal and external event to reach employees, customers, and business partners.	Host a live event in Teams. When you host live events in Teams, you can connect via your camera and share your screen in just a few clicks. Attendees can participate from any browser or device just as easily as attending a Teams meeting, and moderated Q&A and live captions are available to enhance the attendee experience.
Engage a broad internal community or reach employees company-wide on a topic with ongoing engagement.	Host a live event in Yammer. CEO town halls and Ask Me Anything (AMA) events work well in Yammer. You can use webcams and screen-sharing, or for more studio-quality broadcasts, additional production tools can be used.
Deliver internal live or on-demand video for announcements, training, or other specialized topics.	Host a live event in Stream. Live broadcasts can be viewed in Stream or embedded on custom intranet pages or other hosting spots, and when the event ends employees can find them there later. These events also use additional production tools to enable studio-quality broadcasts.

Crisis communications

The Microsoft Power Platform, including Power Automate and Power Apps can be used to communicate with remote workers in a number of ways. For example:

- Microsoft Forms can be used to survey your remote workers and determine:
  - What devices users have at home (type and platform);
  - If users have capable Internet capability at home;
  - If thin clients or desktop and app virtualization can be leveraged for remote workers;
  - If additional user training is needed for remote work scenarios; and
  - If there are any blockers to enabling remote work.
- The free Crisis Communication app can be used to provide your users with a single portal to help ensure they are equipped with recommendations from global health authorities, topical world news, the latest information from government officials and experts, and company-specific content including relevant contacts, company news, and links to support channels. Users can also share their status (such as working from home or out of the office) with their teammates, and automatically send help requests to a dedicated channel in Teams.

Communications site

Another option for organization-wide communication is a crisis management site in SharePoint. This is effectively a SharePoint communication site that is used to share news, reports, status, and other information in a visually compelling format. Communication sites are responsive and can be viewed from anywhere on any device. You can provision a pre-configured crisis management site using this look book design, or you can follow these steps to have a live site up and running within 2 hours.

Communities

Yammer communities can also be used to support remote work and engage people across the organization. Communities connect people across organizational and geographic silos. It's important to give people a common place to gather and to share experience. In a community that brings people together to address a challenge, leaders and members can:

- Share announcements at scale. A community provides a consolidated channel for communication. An announcement reaches members with notifications web, on mobile and in email. The community

promotes quick sharing of information that can bypass corporate bottlenecks even when coming from official channels.

- Share knowledge. A community provides a one-stop-shop for people to ask questions and get answers. Knowledge shared is searchable and discoverable, enabling others to find important information.
- Understand people's needs. Organizations can use polls and can monitor the conversation to gain deeper insights about employees and their needs, which in turn accelerates the development and delivery of communications and solutions that address those needs.
- Reach and engage remote workers wherever they are. Leaders can even conduct live and on-demand events, to broadcast important messages and to answer questions of the community.
- Empower and recognize contribution. Community members can be active participants, contributing ideas, skills, and experience to be part of the solution. Praise can be used to recognize achievements and contribution as the community works through the challenges it faces.

You can use these simple steps to get a Yammer community up and running. Also see the Community Admin Best Practices Guide.

Deployment

Enabling your workforce to work remotely is an ongoing challenge, and that challenge is different for every organization. Use the guidance in the following table to deploy your organization's infrastructure to support remote workers.

If you current infrastructure is…	Do the following (if you haven't already)…
On-premises	1. Connect your on-premises infrastructure to the cloud. Use Azure AD to create an Active Directory domain in the cloud and connect it to your on-premises Active Directory domain. Azure AD Connect integrates your on-premises directories with Azure AD. 2. Enable MFA for all users, including admins: a. Plan your user rollout; b. Define network locations; c. Choose authentication methods; d. Plan your registration policy; e. Plan your Conditional Access policies; f. Plan integration with on-premises systems; g. Implement your plan. 3. Enable remote access to web apps without VPN by using Azure AD Application Proxy for on any on-premises apps published for cloud access. 4. Enable access to other apps and on-premises resources using Azure P2S VPN. 5. Optimize your network infrastructure for remote workers. 6. Empower remote workers by deploying: a. Microsoft Teams b. Microsoft 365 or Microsoft 365 Business, including i. Exchange Online (or Exchange Hybrid) ii. SharePoint and OneDrive iii. Office 365 ProPlus 7. Deploy Windows Virtual Desktop to provide remote access to on-premises apps and critical virtual desktops. 8. Deploy endpoint management technologies to manage devices, PCs and other endpoints. 9. Survey your remote workers to ensure their needs are being addressed, and publish remote worker communication resources, such as:

If you current infrastructure is…	Do the following (if you haven't already)…
	a. a SharePoint communications site; b. a Yammer community; c. a crisis communication site. 10. Share the end-user training resources in this document with your remote workers.
Cloud + on-premises (hybrid)	1. Enable MFA for all users, including admins: a. Plan your user rollout; b. Define network locations; c. Choose authentication methods; d. Plan your registration policy; e. Plan your Conditional Access policies; f. Plan integration with on-premises systems; g. Implement your plan. 2. Enable remote access to web apps without VPN by using Azure AD Application Proxy for on any on-premises apps published for cloud access. 3. Enable access to other apps and on-premises resources using Azure P2S VPN. 4. Optimize your network infrastructure for remote workers. 5. Empower remote workers by deploying: a. Microsoft Teams b. Microsoft 365 or Microsoft 365 Business, including i. Exchange Online - move all mailboxes to Exchange Online to get the maximum feature set ii. SharePoint and OneDrive iii. Office 365 ProPlus 6. Deploy Windows Virtual Desktop to provide remote access to on-premises apps and critical virtual desktops. 7. Deploy endpoint management technologies to manage devices, PCs and other endpoints. 8. Survey your remote workers to ensure their needs are being addressed, and publish remote worker communication resources, such as: a. a SharePoint communications site; b. a Yammer community; c. a crisis communication site. 9. Share the end-user training resources in this document with your remote workers.
Cloud-only	1. Enable MFA for all users, including admins: a. Plan your user rollout; b. Define network locations; c. Choose authentication methods; d. Plan your registration policy; e. Plan your Conditional Access policies; f. Plan integration with on-premises systems; g. Implement your plan. 2. Enable remote access to web apps without VPN by using Azure AD Application Proxy for on any on-premises apps published for cloud access. 3. Enable access to other apps and on-premises resources using Azure P2S VPN. 4. Optimize your network infrastructure for remote workers. 5. Empower remote workers by deploying: a. Microsoft Teams b. Microsoft 365 or Microsoft 365 Business, including i. Exchange Online ii. SharePoint and OneDrive iii. Office 365 ProPlus 6. Deploy Windows Virtual Desktop to provide remote access to on-premises apps and critical virtual desktops.

If you current infrastructure is…	Do the following (if you haven't already)…
	7. Deploy endpoint management technologies to manage devices, PCs and other endpoints. 8. Survey your remote workers to ensure their needs are being addressed, and publish remote worker communication resources, such as: a. a SharePoint communications site; b. a Yammer community; c. a crisis communication site. 9. Share the end-user training resources in this document with your remote workers.

If you need help, Microsoft FastTrack and Microsoft partners are always available to help you establish a productive and secure remote work environment. FastTrack is a benefit that comes with your eligible Microsoft 365 subscription, at no additional cost, and can also be used with the free 6-month Office 365 E1 and G1 trials and the Office 365 A1 student subscription. This is available to customers with 150 or more licenses of the eligible plans or trials. Submit a request for assistance on the FastTrack site.

Training and resources

Below are links to a variety of training materials and resources to help you quickly pivot to a remote workforce. These include resources for IT professionals and end users (including materials for IT pros to distribute to end users).

IT pro training and resources

Use the following training materials and resources to help enable your remote workers to be effective, productive, and connected from home.

Scenario	Resource
Identity	• Top 5 ways your Azure AD can help you enable remote work • Plan and deploy your Microsoft 365 identity infrastructure • Enable sign-in security • Azure Academy Quick Start Videos
Networking	• How to quickly optimize Office 365 traffic for remote staff & reduce the load on your infrastructure • Securely connect to on-prem data and resources • Enable access to on-premises apps, LOB, etc.
Deployment	• Core deployment of foundation infrastructure for Microsoft 365 • Microsoft 365 deployment guide • Deploy productivity apps for managed devices • Deploy Windows 10 to enable comprehensive security features for identity, threat, and information protection
Security	• Zero Trust security vision paper • Secure your mobile email with Microsoft Outlook and EMS • Use tenant restrictions to manage access to SaaS cloud applications • Top 10 ways to secure Office 365 and Microsoft 365 • Getting Started with Securing Microsoft Teams
Desktop virtualization	• WVD Design and Architecture Guide • WVD Deployment Guide • WVD Hands on Lab Guide

Scenario	Resource
Device/app management	• Enroll managed devices for security, leverage app settings for unmanaged devices, and use device and app policies • How to enroll different types of devices for mobile device management (MDM) • How to use mobile application management (MAM) for non-enrolled BYOD devices • How to educate end users about Microsoft Endpoint Manager
Productivity	• Train your users on Office and Office 365 • Use Office for the web • Enable protection of data • SharePoint sites for highly regulated data • Teams Customer Success Kit • Support remote workers using Microsoft Teams • Create a change management strategy for Microsoft Teams • Teams for highly regulated data • Drive user adoption for remote workers • Tools for driving Teams adoption • Transition from Skype for Business to Microsoft Teams: Latest functionality and upgrade resources
Communications	• Set up and learn about the Crisis Communication sample template in Power Apps • Keeping employees informed and engaged during difficult times • Build a crisis management site to connect people and information

End-user training

Deploying productivity apps to your remote workers provides them with the tools necessary to be productive and stay connected to their teammates, but without the proper training and guidance, your users may struggle to collaborate and be productive. Use the resources below to provide training to your remote workers to help them be effective, productive, and connected from home.

Scenario	Resource
Meetings Calls Chat Video conferencing Remote learning	• Install Teams mobile client • 4 Tips for working from home with Microsoft Teams • Six things to know about chat in Microsoft Teams • End user training for Microsoft Teams • Get started with Teams • Run effective meetings with Teams • Learn to use apps in Teams • Get started with Microsoft Teams for remote learning • Teams Overview Welcome video • Teams Quick Start Guide (PDF download) • Teams Quick Start Videos • Meetings in Teams Video
Email Collaboration File sharing	• Modern Workplace Training • Collaborate with Office 365 • Office 365 Training Center • Collaborate from anywhere using Office 365 • Get started with Office for the web in Office 365 • Office apps help and training • Outlook video training • OneDrive video training • SharePoint Online video training